Order Code RL33637

CRS Report for Congress

Electronic Surveillance Modernization Act, as Passed by the House of Representatives

Updated January 18, 2007

Elizabeth B. Bazan
Legislative Attorney
American Law Division

Prepared for Members and Committees of Congress

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
18 JAN 2007	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Electronic Surveillance Modernization Act, as Passed by the House of Representatives	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Congressional Research Service the Library of Congress, 101 Independence Ave SE, Washington, DC 20540-7500**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**44**	

Electronic Surveillance Modernization Act, as Passed by the House of Representatives

Summary

After the *New York Times* reported that the National Security Agency (NSA) was conducting a secret Terrorist Surveillance Program (TSP), a national debate emerged about whether the program was subject to the Foreign Intelligence Surveillance Act (FISA), whether the Administration needed additional authority to continue the program, and how and whether Congress should oversee the program. The TSP involved surveillance without a warrant or court order under FISA of international communications of persons within the United States, where one party to the communication is believed to be a member of al Qaeda, affiliated with al Qaeda, a member of an organization affiliated with al Qaeda, or working in support of al Qaeda. The Bush Administration asserted constitutional and statutory support for its program. While describing electronic surveillance under FISA as a valuable tool in combating terrorism, the Administration argued that it lacked the speed and agility to deal with such terrorists or terrorist groups. In a January 17, 2007, letter to Chairman Leahy and Senator Specter of the Senate Judiciary Committee, Attorney General Gonzales advised them that, on January 10, 2007, a Foreign Intelligence Surveillance Court (FISC) judge "issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization." In light of these orders, which "will allow the necessary speed and agility," he stated that all surveillance previously occurring under the TSP will now be conducted subject to the approval of the FISC. He indicated further that the President has determined not to reauthorize the TSP when the current authorization expires.

The NSA program has been challenged on legal and constitutional grounds. On August 17, 2006, in *American Civil Liberties Union v. National Security Agency*, Case No. 06-CV-10204 (E.D. Mich. August 17, 2006), Judge Taylor held the program unconstitutional and granted a permanent injunction of the Terrorist Surveillance Program. The decision has been appealed to the U.S. Court of Appeals for the Sixth Circuit. On October 4, 2006, the Sixth Circuit granted a motion staying Judge Taylor's judgment and permanent injunction pending appeal.

The Electronic Surveillance Modernization Act, H.R. 5825, 109th Congress, was one of a number of bills introduced in the Senate and the House of Representatives addressing various aspects of the TSP and a variety of approaches to electronic surveillance of terrorists and those affiliated with them. This bill was designed to enhance flexibility in electronic surveillance to acquire foreign intelligence information, while requiring increased reporting and congressional oversight of these activities. The measure was introduced on July 18, 2006, and passed the House on September 28, 2006. This report summarizes the bill as passed by the House and analyzes the potential impact of its provisions were they to become law. The 110th Congress may wish to contemplate similar or different approaches to these issues, or may choose to forego legislation in light of the new FISC orders and the anticipated termination of the TSP, while continuing congressional oversight. This report will not be updated.

Contents

Introduction 1

Sec. 2. FISA Definitions 4
- "Agent of a foreign power" 4
- "Electronic surveillance" 5
- "Minimization procedures" 7
- "Wire communication and surveillance device" 8
- "Contents" 8

Sec. 3. Authorization for Electronic Surveillance and Other Acquisitions for Foreign Intelligence Purposes 8
- Authorization for Electronic Surveillance for Foreign Intelligence Purposes 8
- Authorization for Acquisition of Foreign Intelligence Information 11
- Directives Relating to Electronic Surveillance and Other Acquisitions of Foreign Intelligence Information 12
  - Liability 13
  - Use of information acquired pursuant to directive under proposed section 102B 14
  - Use of information acquired under proposed section 102B in law enforcement 14
  - Disclosure by the government in federal proceedings of information acquired under section 102 or 102A 14
  - Disclosure in state or local proceedings of information obtained or derived under proposed section 102 or 102A 14
  - Motion to exclude evidence obtained or derived under proposed section 102 or 102A 14
  - Review of motions 15

Sec. 4. Jurisdiction of FISA Court 19

Sec. 5. Applications for Court Orders 20

Sec. 6. Issuance of an Order 22
- Necessary Findings 22
- Specifications Required 23
- Striking of Provision Dealing with Exclusion From FISA Electronic Surveillance Orders of Information Regarding Foreign Power Targets 24
- Duration and Extension of Orders for Electronic Surveillance Under FISA 25
- Emergency Electronic Surveillance Prior to FISC Order 25
- Release From Liability 26
- Authorization of Pen Registers and Trap and Trace Devices Where Electronic Surveillance Involving Communications Authorized Under FISA 27

Sec. 7. Use of Information 27

Sec. 8. Congressional Oversight 28

Sec. 9. International Movement of Targets 32
Electronic Surveillance Under FISA 32
Physical Searches Under FISA 32

Sec. 10. Compliance with Court Orders and Antiterrorism Programs 33

Sec. 11. Report on Minimization Procedures 34

Sec. 12. Authorization After an Armed Attack 34
Warrantless Electronic Surveillance for Limited Period Under FISA 34
Warrantless Physical Search for Limited Period Under FISA 35

Sec. 13. Authorization of Electronic Surveillance After a Terrorist Attack 35
Initial Authorization 35
Subsequent Certifications 36
Electronic Surveillance of Individuals 36
Minimization Procedures 37
Electronic Surveillance of United States Persons 37
Use of Information 37
Reporting Requirements 37

Sec. 14. Authorization of Electronic Surveillance Due to Imminent Threat . . . 38
Initial Authorization 38
Subsequent Authorizations 38
Electronic Surveillance of Individuals 39
Minimization Procedures
. 39
Electronic Surveillance of United States Persons 39
Use of Information Acquired by Electronic Surveillance Under
This Section 39

Sec. 15. Technical and Conforming Amendments 40

Electronic Surveillance Modernization Act, as Passed by the House of Representatives

Introduction

After the *New York Times* reported that the National Security Agency (NSA) was conducting a secret Terrorist Surveillance Program (TSP), a national debate emerged about whether the program was subject to the Foreign Intelligence Surveillance Act (FISA), whether the Administration needed additional authority to continue the program, and how and whether Congress should oversee the program. The TSP involved surveillance without a warrant or court order under the FISA of international communications of persons within the United States, where one party to the communication is believed to be a member of al Qaeda, affiliated with al Qaeda, a member of an organization affiliated with al Qaeda, or working in support of al Qaeda. The Bush Administration asserted constitutional and statutory support for its program.

The Foreign Intelligence Surveillance Act, P.L. 95-511, Title I, October 25, 1978, 92 Stat. 1796, codified at 50 U.S.C. § 1801 *et seq.*, as amended, provides a statutory framework for the use of electronic surveillance, physical searches, pen registers and trap and trace devices to acquire foreign intelligence information.[1] It

---

[1] Under section 101(e) of FISA, 50 U.S.C. § 1801(e), "foreign intelligence information" is defined to mean:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against —
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to —
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

"United States person" is defined in subsection 101(i) of FISA, 50 U.S.C. § 1801(c) to mean "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in

(continued...)

also provides statutory authority for the production of tangible things for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.[2] While describing electronic surveillance under FISA as a valuable tool in combating terrorism, the Bush Administration argued that it lacked the speed and agility to deal with such terrorists or terrorist groups.[3]

In a January 17, 2007, letter to Chairman Leahy and Senator Specter of the Senate Judiciary Committee, Attorney General Gonzales advised them that, on January 10, 2007, a Foreign Intelligence Surveillance Court (FISC) judge "issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization." The Attorney General stated that, in light of these orders, which "will allow the necessary speed and agility," all surveillance previously occurring under the TSP will now be conducted subject to the approval of the FISC. He indicated further that, under these circumstances, the President has determined

---

[1] (...continued)
subsection (a)(1), (2), or (3) of this section."

"International terrorism" is defined in subsection 101(c), 50 U.S.C. § 1801(c) to mean activities that:

> (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
> (2) appear to be intended —
> (A) to intimidate or coerce a civilian population;
> (B) to influence the policy of a government by intimidation or coercion; or
> (C) to affect the conduct of a government by assassination or kidnapping; and
> (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

"Sabotage" is defined in 50 U.S.C. § 1801(d) to mean "activities that involve a violation of chapter 105 of Title 18, or that would involve such a violation if committed against the United States."

[2] Under Sec. 106(a)(1) of FISA, 50 U.S.C. § 1861(a)(1), where such an investigation is of a United States person, it may not be conducted "solely upon the basis of activities protected by the first amendment to the Constitution."

[3] *See* U.S. DEPARTMENT OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT 34 (January 19, 2005); Letter of December 22, 2005, from Assistant Attorney General William E. Moschella to the Honorable Pat Roberts, the Honorable John D. Rockefeller, IV, the Honorable Peter Hoekstra, and the Honorable Jane Harman, at 5; Statements by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, during December 19, 2005, Press Briefing available at [http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html].

not to reauthorize the TSP when the current authorization expires. The Attorney General also noted that the Intelligence Committees had been briefed on the highly classified details of the FISC orders and advised Chairman Leahy and Senator Specter that he had directed the Acting Assistant Attorney General for the Office of Legal Counsel and the Assistant Attorney General for National Security to provide them a classified briefing on the details of the orders.

The NSA program has been challenged on legal and constitutional grounds. On August 17, 2006, in one such lawsuit, *American Civil Liberties Union v. National Security Agency*, Case No. 06-CV-10204 (E.D. Mich. August 17, 2006), U.S. District Court Judge Anna Diggs Taylor held the program unconstitutional on the ground that it violated the Administrative Procedures Act, the Separation of Powers doctrine, the First and Fourth Amendments of the U.S. Constitution, the Foreign Intelligence Surveillance Act (FISA), and Title III of the Omnibus Crime Control and Safe Streets Act (Title III), and permanently enjoined the Terrorist Surveillance Program. The decision has been appealed to the U.S. Court of Appeals for the Sixth Circuit. On October 4, 2006, the Sixth Circuit stayed Judge Taylor's August 17, 2006, judgment and permanent injunction pending appeal, *American Civil Liberties Union v. National Security Agency*, Docket Nos. 06-2140 and 06-2095 (6th Cir. Oct. 4, 2006). The docket sheets for both Docket Nos. 06-2140 and 06-2095 indicate that a letter from the attorneys for the appellants was filed on January 18, 2007, notifying the court "concerning a letter from the Attorney General's Office regarding orders issued by the Foreign Intelligence Surveillance Court."

Several bills were introduced in the 109th Congress to amend the Foreign Intelligence Surveillance Act and to address concerns raised with respect to the Terrorist Surveillance Program. One of these bills, the Electronic Surveillance Modernization Act, H.R. 5825, 109th Congress, was introduced on July 18, 2006, and passed the House on September 28, 2006.[4] The measure was designed to provide

---

[4] H.R. 5825, the Electronic Surveillance Modernization Act, was introduced on July 18, 2006, by Representative Heather Wilson, for herself, Representative Sensenbrenner, Representative Hoekstra, Representative Renzi, Representative Johnson of Connecticut, Representative Everett, Representative Thornberry, Representative Rogers of Michigan, Representative Gallegly and Representative Issa. The bill was referred the same day to both the House Committee on the Judiciary and to the House Permanent Select Committee on Intelligence. On September 1, 2006, it was referred to the Subcommittee on Crime, Terrorism, and Homeland Security of the House Judiciary Committee. On September 20, 2006, the House Judiciary Committee ordered the bill to be reported out amended by a vote of 20 yeas-16 nays. The House Permanent Select Committee on Intelligence approved an amended version of the bill by voice vote in a closed session the same day. On September 25, 2006, the bill was reported out, amended, from both the House Permanent Select Committee on Intelligence (H.Rept. 109-680, Part I) and the House Judiciary Committee (H.Rept. 109-680, Part II), and the measure was placed on the Union Calendar, Calendar No. 410. On September 28, 2006, the House Committee on Rules reported H.Res. 1052 to the House, providing for consideration of H.R. 5825. In lieu of the amendments recommended by the House Permanent Select Committee on Intelligence and the House Judiciary Committee, the Rules Committee reported H.Amdt. 1214, an amendment in the nature of a substitute which was considered as adopted pursuant to H.Res. 1052. At 10:18 p.m. that evening, H.R. 5825, as so amended, passed the House of Representatives by a vote of 232

(continued...)

increased flexibility in authorizing electronic surveillance to acquire foreign intelligence information, while requiring increased reporting and affording Congress additional oversight over such activities. The 110th Congress may choose to explore similar or different approaches to the issues related to the TSP,[5] or may choose to forego legislative action in light of the new FISC orders and the anticipated termination of the TSP at the conclusion of its current authorization, while continuing congressional oversight of these issues.

This report summarizes the provisions of H.R. 5825, as passed by the House of Representatives in the 109th Congress,[6] and discusses the impact of its provisions, were similar legislation to be enacted, on current law. The sections of the bill are addressed in the order in which they appear in the bill.

Sec. 2. FISA Definitions

Sec. 2 of the bill amends several of the current definitions in the Foreign Intelligence Surveillance Act (FISA).

"Agent of a foreign power"

Sec. 2(a) amends definition of "agent of a foreign power" in subsection 101(b)(1), 50 U.S.C. § 1801(b)(1),[7] to add a new category covering any person, other

---

[4] (...continued)
to 191 (Roll No. 502).

[5] Three related bills have been introduced to date in the 110th Congress: H.R. 11, the NSA Oversight Act, introduced by Representative Schiff, for himself and Representative Flake, Representative Van Hollen, Representative Inglis of South Carolina, Representative Inslee, and Representative Mack, on January 4, 2007, and referred to the House Committee on the Judiciary, and, in addition, to the House Permanent Select Committee on Intelligence, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned; S. 187, the Foreign Intelligence Surveillance Oversight and Resource Enhancement Act of 2007, introduced by Senator Specter on January 4, 2007, and referred to the Senate Committee on the Judiciary; and S. 139, the Foreign Surveillance Expedited Review Act, introduced by Senator Schumer on January 4, 2007, and referred to the Senate Committee on the Judiciary.

[6] Unless otherwise indicated, H.R. 5825, as used in this report, refers to H.R. 5825 as passed by the House of Representatives.

[7] Under current law, "agent of a foreign power," as defined in subsection 101(b)(1) of FISA, 50 U.S.C. § 1801(b)(1), includes three categories of persons who are not United States persons. These categories include any person other than a United States person, (A) who acts in the United States as an officer or employee of a foreign power, or, as a member of a group engaged in international terrorism or activities in preparation therefor; (B) who acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in (continued...)

than a United States person,[8] who "(D) is reasonably expected to possess, control, transmit, or receive foreign intelligence information while such person is in the United States, provided that the official making the certification required by section 104(a)(7) deems such foreign intelligence information to be significant." Unlike the definitions of "agent of a foreign power" in subsections 101(b)(1)(A) and 101(b)(1)(B) of FISA, but like the so-called "lone wolf" provision in subsection 101(b)(1)(C) of FISA, the definition of an "agent of a foreign power" under proposed subsection 101(b)(1)(D) does not require that the non-U.S. person covered by this new definition have any connection with a foreign power. However, it differs from the latter provision in that under proposed subsection 101(b)(1)(D), a reasonable expectation that a non-U.S. person will possess foreign intelligence information, without more, appears sufficient for that person to be categorized as an "agent of a foreign power." In addition, under the proposed new definition, a non-U.S. person who is "reasonably expected to control, transmit, or receive foreign intelligence information while in the United States" would also be considered an "agent of a foreign power." The proposed definition does not appear to require an action or intent to act for the benefit of a foreign power or against the interests of the United States, nor does it require any ill intent. This would seem to significantly broaden the reach of the term so defined.

"Electronic surveillance"

Sec. 2(b) amends the definition of "electronic surveillance" in subsection 101(f) of FISA, 50 U.S.C. § 1801(f), to mean:

> (1) the installation or use of an electronic, mechanical, or other surveillance device [as defined in subsection (2)(d) of the bill, new subsection 101(*l*) of FISA, 50 U.S.C. § 1801(*l*)[9]] for acquiring information by intentionally directing

---

[7] (...continued)
the conduct of such activities or knowingly conspires with any person to engage in such activities; or (C) who engages in international terrorism or activities in preparation for international terrorism.

[8] Under section 101(i) of FISA, 50 U.S.C. § 1801(i), a "United States person" is defined to mean "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act [8 U.S.C. § 1101(a)(20)]), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section." Under the cross-referenced sections, "foreign power" means "a foreign government or any component thereof, whether or not recognized by the United States;" "a faction of a foreign nation or nations, not substantially composed of United States persons;" or "an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments." It does not include international terrorist organizations.

[9] Under current law, subsection 101(*l*) of FISA, 50 U.S.C. § 1801(l) defines "wire communication" to mean, "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in (continued...)

> surveillance at a particular known person who is reasonably believed to be in the United States, under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; or
> (2) the intentional acquisition of the contents of any communication under circumstances in which a person has reasonable expectation of privacy and a warrant would be required for law enforcement purposes, if both the sender and all intended recipients are reasonably believed to be located within the United States.[10]

Although this is a broader, shorter, and more general definition than that contained in current law, there are some similarities in language.

Proposed subsection 101(f)(1) blends some of the elements of current subsections 101(f)(1) and (f)(4) with new elements, while eliminating other aspects of those provisions. Current subsection 101(f)(1) deals with the use of a surveillance device to intercept the contents of wire or radio communications sent by or intended to be received by a particular, known, intentionally targeted U.S. person, who is in

---

[9] (...continued)
providing or operating such facilities for the transmission of interstate or foreign communications." Under the new definition of "surveillance device" in Sec. 2(d) of H.R. 5825, the term would mean, "a device that allows surveillance by the Federal Government, but excludes any device that extracts or analyzes information from data that has already been acquired by the Federal Government by lawful means." While the term "surveillance device" is not currently defined in FISA, it is used in the current definition of "electronic surveillance" under subsection 101(f) of FISA, 50 U.S.C. § 1801(f).

[10] Under current law, "electronic surveillance" is defined under subsection 101(f) of FISA, 50 U.S.C. § 1801(f), to mean:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;
> (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

the United States, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. Current subsection 101(f)(4) deals with the installation or use of a surveillance device in the United States "for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." However, unlike current subsection 101(f)(1), the new definition does not explicitly distinguish between interception of the communications of U.S. persons and those of non-U.S. persons, nor is it restricted to acquisition of the contents of communications. The current subsection 101(f)(1) requires the person intentionally targeted to be in the United States, while the proposed provision requires a reasonable belief that the person at whom surveillance is intentionally directed be in the United States. Both proposed subsection 101(f)(1) and current subsection 101(f)(4) deal with the installation or use of an electronic, mechanical, or other surveillance device to acquire information, but unlike current subsection 101(f)(4), the proposed definition contains no express requirement that the surveillance device be installed or used in the United States, and no restriction on acquisition of that information from wire or radio communications. The proposed subsection 101(f)(1) explicitly involves intentionally directing surveillance at a particular known person, while current subsection 101(f)(4) does not.

Proposed subsection 101(f)(2) has significant parallels to current subsection 101(f)(3), in that both deal with "intentional acquisition" of the contents of a "communication under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." However, the current provision is limited to intentional acquisition of radio communications by means of "an electronic, mechanical, or other surveillance device." The proposed provision is not so limited, applying to the intentional acquisition of "any communication," without limiting it to radio communications or expressly restricting the means by which the acquisition occurs. The current provision requires that "both the sender and all the intended recipients are located in the United States," while the bill's provision requires that both the sender and all intended recipients be reasonably believed to be located within the United States.

"Minimization procedures"

Under current law, "minimization procedures" are defined in section 101(h) of FISA, 50 U.S.C. § 1801(h)(1)-(4). Sec. 2(c)(3) of H.R. 5825 amends the definition of "minimization procedures" in section 101(h), 50 U.S.C. § 1801(h), to delete subsection (4). Current subsection 101(h)(4) of FISA, 50 U.S.C. § 1801(h)(4), includes in the definition of "minimization procedures," with respect to any electronic surveillance approved pursuant to 50 U.S.C. § 1802(a),[11] "procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under [section 105 of FISA, 50 U.S.C. § 1805,] is

[11] See the discussion of current section 102 of FISA and proposed sections 102, 102A, and 102B of FISA under H.R. 5825 in the discussion of Sec. 3 of H.R. 5825, *infra*.

obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person."

"Wire communication and surveillance device"

Sec. 2(d) of the bill replaces current definition of "wire communication" in section 101(*l*) with a definition of "surveillance device," which means "a device that allows surveillance by the Federal Government, but excludes any device that extracts or analyzes information from data that already has been acquired by the Federal Government by lawful means."[12]

"Contents"

Sec. 2(e) of H.R. 5825 amends subsection 101(n) of FISA, 50 U.S.C. § 1801(n),[13] when used with respect to a communication, to include "any information concerning the substance, purport, or meaning of that communication."

Sec. 3. Authorization for Electronic Surveillance and Other Acquisitions for Foreign Intelligence Purposes

Authorization for Electronic Surveillance for Foreign Intelligence Purposes

Sec. 3 of H.R. 5825 amends section 102 of FISA, 50 U.S.C. § 1802, by striking the current language and replacing it with a new section 102 of FISA, which contains both similarities to and differences from current law. Under Sec. 3(a) of the bill, new subsection 102(a) of FISA provides that the President, acting through the Attorney General, may authorize electronic surveillance without a court order under title I of FISA,[14] to acquire foreign intelligence information for periods of up to one year, if the Attorney General certifies in writing under oath that the electronic surveillance is directed at acquisition of the contents of communications of a "foreign power," as defined in section 101(a)(1), (2), or (3) of FISA, 50 U.S.C. § 1801(a)(1), (2), or (3), or an "agent of a foreign power" as defined in section 101(b)(1)(A) or (B), 50 U.S.C. § 1801(b)(1)(A) or (B); or at the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 101(a)(1), (2) or (3) of FISA.

---

[12] For further discussion of these definitions, see footnote 7, *supra*.

[13] Under the current Section 101(n) of FISA, 50 U.S.C. § 1801(n), "contents," "when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication."

[14] Title I of FISA is codified at 50 U.S.C. § 1801 *et seq*.

A "foreign power" as defined in section 101(a)(1), (2), or (3) of FISA, 50 U.S.C. § 1801(a)(1), (2), or (3), means a foreign government or any component thereof, whether or not recognized by the United States; a faction of a foreign nation or nations, not substantially composed of United States persons; or an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments. As defined in section 101(b)(1)(A) or (B) of FISA, 50 U.S.C. § 1801(b)(1)(A) or (B), a person who is not a U.S. person is an "agent of a foreign power" if he or she:

> (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4)[15] of this section;
> (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities[.][16]

Proposed subsection102(a)(2) requires that the proposed minimization procedures regarding such a surveillance must meet the definition of minimization procedures

---

[15] Under current Section 101(a)(4) of FISA, 50 U.S.C. § 1801(a)(4), the term "foreign power" is defined to include "a group engaged in international terrorism or activities in preparation therefor[.]"

[16] Under the current section 102(a) of FISA, 50 U.S.C. § 1802(a), the President, through the Attorney General, may authorize electronic surveillance without a court order under FISA to acquire foreign intelligence information for periods of up to one year based upon a written certification under oath by the Attorney General that meets certain criteria and satisfies specified reporting requirements. Under these criteria, the Attorney General must certify that the electronic surveillance is *solely* directed at either the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 101(a)(1), (2) or (3) of FISA, 50 U.S.C. § 1801(a)(1), (2), or (3); or the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as so defined. (Emphasis added.) Under the cross-referenced sections, "foreign power" means a foreign government or any component thereof, whether or not recognized by the United States; a faction of a foreign nation or nations, not substantially composed of United States persons; or an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments. It does not include international terrorist organizations. Current section 102 of FISA does not cover electronic surveillance directed at the acquisition of the contents of communications of an "agent of a foreign power" as defined in subsections 101(b)(1)(A) or (B) of FISA, 50 U.S.C. § 1801(b)(1)(A) or (B). Subsection 101(b)(1)(A) of FISA covers an agent of a foreign power who is not a U.S. person who acts in the United States as an officer or employee of a foreign power as a member of a group engaged in international terrorism or in activities in preparation therefor. Subsection 101(b)(1)(B) of FISA deals with an agent of a foreign power who is not a U.S. person who acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to United States interests when the circumstances of that person's presence in the United States indicates that he or she may engage in such activities in the United States or may aid or abet or conspire with someone engaging in such activities.

under section 101(h) (as amended by Sec. 2(c)(3) of H.R. 5825, discussed above). As under current subsection 102(a) of FISA, 50 U.S.C. § 1802(a), the proposed subsection 102(a) of FISA, as amended by Sec. 3(a) of H.R. 5825, would require the Attorney General to report such minimization procedures and any changes thereto to the congressional intelligence committees at least 30 days prior to the effective date of those procedures, unless he determines that immediate action is required and notifies those committees immediately of the minimization procedures and the reason for their going into effect immediately.

Under current subsection 102(a)(1)(B) of FISA the Attorney General is required, in authorizing electronic surveillance without a court order under section 102 of FISA, 50 U.S.C. § 1802, to certify that "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party." Sec. 3(a) of H.R. 5825 contains no such requirement in the new section 102 of FISA.

Both current section 102(a)(2) of FISA, 50 U.S.C. § 1802(a)(2), and the proposed subsection 102(b) of FISA requires electronic surveillance authorized under section 102 to be conducted only in accordance with the Attorney General's certification and minimization procedures. Both provisions also direct the Attorney General to assess compliance with such minimization procedures and to report those assessments to the congressional intelligence committees under the provisions of section 108(a) of FISA, 50 U.S.C. § 1808(a).

Both current section 102(a)(3) of FISA, 50 U.S.C. § 1802(a)(3), and the proposed subsection 102(c) of FISA require the Attorney General to immediately transmit under seal to the Foreign Intelligence Surveillance Court (FISC)[17] a copy of his certification, which shall be maintained under security procedures established by the Chief Justice of the United States with concurrence of the Attorney General, in consultation with the Director of National Intelligence (DNI). The copy of the Attorney General's certification is to remain sealed unless an application for a court

---

[17] This court was established under section 103(a) of FISA, 50 U.S.C. § 1803(a). The FISC is composed of 11 U.S. district court judges publicly designated by the Chief Justice of the United States from seven circuits, at least three of whom must reside within 20 miles of the District of Columbia. The FISC has jurisdiction to hear applications for court orders authorizing of electronic surveillance or physical searches to obtain foreign intelligence information under FISA. Either an FISC judge, or a U.S. Magistrate Judge publicly designated by the Chief Justice to act on behalf of such judge, may hear applications for and grant orders approving installation and use of pen registers and trap and trace devices or production of any tangible thing for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution. The government may seek review of a denial of an application for a court order authorizing such electronic surveillance, physical search or production of any tangible thing before the Court of Review. If the denial is upheld by the Court of Review, the government may seek U.S. Supreme Court review of the decision under a petition for certiorari.

order with respect to the surveillance is made under section 104 of FISA,[18] 50 U.S.C. § 1804; or unless the certification is necessary to determine the legality of the surveillance under section 106(f) of FISA, 50 U.S.C. § 1806(f).

Authorization for Acquisition of Foreign Intelligence Information

Sec. 3(a) of H.R. 5825 also creates a new Sec. 102A, which, notwithstanding any other law, permits the President, acting through the Attorney General, to authorize, for periods of up to one year, acquisition of foreign intelligence information concerning a person reasonably believed to be outside the United States, if the Attorney General certifies in writing under oath that four criteria are met. These include:

> (1) the acquisition does not constitute electronic surveillance;
> (2) the acquisition involves obtaining the foreign intelligence information from or with the assistance of a wire or electronic communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to wire or electronic communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications;
> (3) a significant purpose of the acquisition is to obtain foreign intelligence information; and
> (4) the proposed minimization procedures with respect to such acquisition activity meet the definition of minimization procedures under section 101(h).

The certification need not identify specific facilities, places, premises, or property at which the acquisition of foreign intelligence information under the proposed section 102A of FISA would be directed.

Although this provision does not address electronic surveillance, like the current and proposed section 102 of FISA, proposed section 102A requires the Attorney General to immediately transmit under seal a copy of his certification to the FISC. The certification would be maintained under security measures established by the Chief Justice and the Attorney General, in consultation with the DNI, and would remain sealed unless the certification is needed to determine the legality of the acquisition under a new section 102B of FISA. The section 102A requirements for conducting such acquisition of foreign intelligence information in accordance with the Attorney General's certification and minimization procedures adopted by him, and for his reporting of assessments of compliance with such minimization procedures to the congressional intelligence committees under section 108(a) of FISA parallel those applicable to the current and proposed section 102 of FISA, discussed above.

---

[18] Under current law, such a certification may also be unsealed if an application for a court order with respect to the surveillance is made under section 101(h)(4) of FISA, 50 U.S.C. § 1801(h)(4). The latter provision would be deleted from FISA under H.R. 5825, Sec. 2(c)(3), discussed above.

Directives Relating to Electronic Surveillance and Other Acquisitions of Foreign Intelligence Information

Pursuant to current subsection 102(a)(4) of FISA, 50 U.S.C. § 1802(a)(4), with respect to electronic surveillance authorized by subsection 102(a) of FISA, the Attorney General may direct a specified communication carrier to "(A) furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers;" and "(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the surveillance or the aid furnished which such carrier wishes to retain." The government is also directed to compensate the communications carrier at the prevailing rate for furnishing such aid.

Sec. 3(a) of H.R. 5825 creates a new section 102B of FISA, concerning directives relating to electronic surveillance and other acquisitions of foreign intelligence information. Under this proposed section, with respect to either an authorization of electronic surveillance under new section 102 or an authorization of acquisition of foreign intelligence information under section 102A, the Attorney General may direct any person to immediately provide the government with all information, facilities, and assistance necessary to accomplish the acquisition of foreign intelligence information in a manner which will protect the secrecy of the electronic surveillance or acquisition and produce a minimum of interference with customer services. The Attorney General may require such person to maintain any records he or she wishes to retain concerning such electronic surveillance or acquisition, or the aid provided, under security procedures approved by the Attorney General and the DNI.[19] In addition, the proposed subsection 102B of FISA would authorize compensation by the government to a person providing such information, facilities, or assistance at the prevailing rate.[20]

Should a person or entity fail to comply with a directive issued under new section 102B(a) of FISA, the Attorney General may petition the FISC to compel compliance. The FISC shall order compliance with the directive if it finds that the directive was issued pursuant to proposed sections 102(a) or 102A(a) and is otherwise lawful. Failure to comply with such a court order may be punished as contempt of court. Related process may be served in any judicial district in which the person or entity is found.[21]

A person receiving a directive under section 102B(a) may challenge its legality by filing a petition under seal before the petition review pool of the FISC established under subsection 103(e)(1) of FISA.[22] Such petitions are assigned to judges of the

---

[19] Proposed subsection 102B(a) of FISA, Sec. 3(a) of H.R. 5825.

[20] Proposed subsection 102B(b) of FISA, Sec. 3(a) of H.R. 5825.

[21] Proposed subsection 102B(c) of FISA, Sec. 3(a) of H.R. 5825.

[22] Proposed subsection 102B(d) of FISA, Sec. 3(a) of H.R. 5825. This petition review pool, established under section 103(e)(1) of FISA and there given jurisdiction to review petitions

(continued...)

FISC petition review pool by the presiding judge of the Foreign Intelligence Surveillance Court of Review (Court of Review). An initial review must be conducted by the judge assigned to a petition within 24 hours of assignment. If the petition is deemed frivolous, the judge will deny the petition and affirm the directive or any part thereof that is the subject of the petition. If the petition is not deemed frivolous, the judge has 72 hours within which to make a determination on a petition and to provide a written statement for the record of his or her reasons for that determination.[23] A petition to modify or set aside a directive may only be granted if the judge finds that the directive does not meet the requirements of this section or is otherwise unlawful. Otherwise, the judge must affirm the directive and order the recipient to comply with it. Unless modified or set aside, a directive under this section is to remain in full effect.[24]

The government or any person receiving the petition has seven days to appeal a decision regarding that petition to the Court of Review, which shall provide a written statement for the record of the reasons for its decision. Recourse to the U.S. Supreme Court by certiorari petition may be sought by the government or any person receiving the petition for review of the Court of Review's decision. The record below shall be transmitted to the U.S. Supreme Court under seal.[25]

All petitions under section 102A are to be filed under seal. In any proceedings under this section, upon request of the government, the court shall review *ex parte* and *in camera* any submission, or part of a submission, by the government that may contain classified information.[26]

Liability. No person providing any information, facilities, or assistance pursuant to such a directive may be subject to suit for such compliance.[27]

---

[22] (...continued)
filed under section 501(f)(1) of FISA, 50 U.S.C. § 1861(f)(1), is made up of three FISC judges who reside within 20 miles of the District of Columbia, or, if all of such judges are unavailable, other FISC judges, designated by the FISC presiding judge to serve in the pool. Under subsection 103(e)(2), by May 8, 2006, the FISC court was required to adopt and, consistent with the protection of national security, to publish procedures for the review of petitions filed pursuant to section 501(f)(1) of FISA, 50 U.S.C. §1861(f)(1), by the petition review panel. Such procedures are required to provide that review of a petition shall be conducted *in camera* and shall also provide for the designation of an acting presiding judge. *See* PROCEDURES FOR REVIEW OF PETITIONS FILED PURSUANT TO SECTION 501(F) OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (effective May 5, 2006), which may be found at [http://www.uscourts.gov/rules/FISA_Procedures.pdf].

[23] The review of a petition challenging the legality of a directive under section 102B is to be conducted pursuant to procedures issued under section 103(e)(2) for review petitions filed under section 501(f)(1) of FISA, 50 U.S.C. § 1861(f)(1).

[24] Proposed subsection 102B(d) of FISA, Sec. 3(a) of H.R. 5825.

[25] Proposed subsection 102B(e) of FISA, Sec. 3(a) of H.R. 5825.

[26] Proposed subsection 102B(g) of FISA, Sec. 3(a) of H.R. 5825.

[27] Proposed subsection 102B(h) of FISA, Sec. 3(a) of H.R. 5825.

Use of information acquired pursuant to directive under proposed section 102B. Information acquired pursuant to a new section 102B directive concerning a U.S. person may only be used and disclosed by federal officers or employees without that U.S. person's consent in accordance with minimization procedures required by proposed sections 102(a) and 102A(a) of FISA. Otherwise privileged communications obtained in accordance with, or in violation of, proposed sections 102, 102A, or 102B of FISA retain their privileged character. Information from an electronic surveillance pursuant to proposed section 102 of FISA or an acquisition of foreign intelligence information under proposed section 102A of FISA may only be used or disclosed by federal officers or employees for lawful purposes.[28]

Use of information acquired under proposed section 102B in law enforcement. Information acquired pursuant to proposed section 102B of FISA may only be disclosed for law enforcement purposes if the disclosure is accompanied by a statement that such information, and any derivative information, may only be used in a criminal proceeding with advance authorization of the Attorney General.[29]

Disclosure by the government in federal proceedings of information acquired under section 102 or 102A. If the federal government intends to enter into evidence or otherwise use or disclose information obtained or derived from an electronic surveillance under proposed section 102 of FISA or an acquisition under proposed section 102A of FISA in any federal trial, hearing or proceeding against an aggrieved person, the government must notify the aggrieved person and the court or other authority in which the information is to be disclosed or used of the government's intention, prior to that trial, hearing or proceeding or at a reasonable time prior to an effort to submit that information in evidence or to use or disclose it.[30]

Disclosure in state or local proceedings of information obtained or derived under proposed section 102 or 102A. Should a state or political subdivision of a state seek to enter into evidence or otherwise use or disclose against an aggrieved person information obtained or derived from electronic surveillance under proposed section 102 of FISA or from an acquisition of foreign intelligence information under proposed section 102A of FISA, H.R. 5825 requires the state or political subdivision to notify the aggrieved person, the court or other authority involved, and the U.S. Attorney General of its intention.[31]

Motion to exclude evidence obtained or derived under proposed section 102 or 102A. A person against whom such evidence is to be or has been used or disclosed in any federal, state, or local trial, hearing, or other proceeding may move to suppress the evidence so obtained or derived on the grounds that the information was unlawfully acquired or the electronic surveillance or acquisition of foreign intelligence information was not made in conformity with an authorization

---

[28] Proposed subsection 102B(i) of FISA, Sec. 3(a) of H.R. 5825.

[29] Proposed subsection 102B(j) of FISA, Sec. 3(a) of H.R. 5825.

[30] Proposed subsection 102B(k) of FISA, Sec. 3(a) of H.R. 5825.

[31] Proposed subsection 102B(*l*) of FISA, Sec. 3(a) of H.R. 5825.

under proposed section 102(a) or 102A(a) of FISA. Such a motion must be made before the trial or proceeding, unless there was no opportunity to make such a motion or that person was unaware of the grounds for the motion.[32]

Review of motions. Proposed subsection 102B(n) provides a mechanism for review if a federal, state or local court or authority is notified under proposed subsections 102B(k) or (*l*) of FISA of intended use or disclosure of information obtained or derived under proposed section 102 or 102A; if a section 102B(m) motion is filed to suppress the evidence or information so obtained or derived; or if a motion or request is filed by an aggrieved person under any other federal or state statute before a federal or state court or authority either to discover or obtain an Attorney General directive or other materials related to an electronic surveillance under proposed section 102 or an acquisition of foreign intelligence information under proposed section 102A, or to discover, obtain, or suppress evidence or information obtained or derived under proposed section 102 or 102A.[33] Notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm U.S. national security, then either the U.S. district court in which the notice, motion or request is filed, or, if made before another authority, the U.S. district court in the same district as that authority will review *in camera* and *ex parte* the application, order and such other material pertaining to the electronic surveillance or acquisition of foreign intelligence information at issue to determine whether the electronic surveillance or the acquisition was lawfully authorized and conducted. In making this determination, where necessary to accurately determine the legality of the acquisition, the court may, under appropriate security procedures and protective orders, disclose portions of the directive or other materials relating to that acquisition to the aggrieved person.[34]

---

[32] Proposed subsection 102B(m) of FISA, Sec. 3(a) of H.R. 5825.

[33] Proposed subsection 102B(n) of FISA speaks in terms of review of "motions," although the introductory language of the section also refers to notifications under proposed sections 102B(k) or (*l*) of FISA and to requests (as well as motions) made by an aggrieved person pursuant to any other statute or rule of the United States or any state before any court or authority of the United States or any state (1) to discover or obtain an Attorney General directive or other materials relating to an electronic surveillance under proposed section 102 of FISA or an acquisition under proposed section 102A of FISA; or (2) to discover, obtain, or suppress evidence or information obtained or derived from an electronic surveillance under proposed section 102 of FISA or an acquisition under proposed section 102A of FISA.

[34] Proposed subsection 102B(n) of FISA, Sec. 3(a) of H.R. 5825. Under the language of the bill, disclosure of portions of the directive or other material relating to the *acquisition* may be made to the aggrieved person only when necessary to make an accurate determination of the *acquisition*'s legality. [Emphasis added.] There is no parallel language in this subsection expressly limiting such disclosure of portions of the directive or other material relating to an electronic surveillance under section 102 where necessary to determine that electronic surveillance's legality. It is not clear whether "acquisition" in this instance is intended to cover both electronic surveillance under proposed section 102 of FISA and acquisition of foreign intelligence information by means other than electronic surveillance under proposed section 102A of FISA, or whether it is intended only to cover the latter. Although Sec. 3 of the bill is entitled "Authorization for Electronic Surveillance and Other Acquisitions for Foreign Intelligence Purposes," FISA, as amended by H.R. 5825, has no similar heading.
(continued...)

Under proposed subsection 102B(o) of FISA, if the court finds the acquisition[35] was not lawfully authorized or conducted, then evidence obtained or derived from that acquisition shall be suppressed or the motion of the aggrieved person shall be otherwise granted. If the acquisition is found to be lawfully authorized and

---

[34] (...continued)
The Sec. 3 heading would lend support to an interpretation that "acquisition" here may be intended to cover both electronic surveillance under proposed section 102 of FISA and other acquisitions of foreign intelligence information under proposed section 102A of FISA. On the other hand, the earlier language of this subsection treats both electronic surveillance under section 102 and acquisition of foreign intelligence information under section 102A explicitly, while the latter part of the subsection speaks only to "acquisition." This might tend to support an interpretation that the latter use of "acquisition" was advised and was intended to cover only acquisitions under section 102A.

Some support for a more inclusive interpretation of the term "acquisition" might also be drawn from proposed subsection 102B(q), which deals with consultation by federal officers who acquire foreign intelligence information with federal law enforcement officers and state, and local law enforcement personnel to coordinate efforts to investigate or protect against certain categories of actions. Proposed subsection 102B(q)(1) permits such consultation. Proposed subsection 102B(q)(2) provides that coordination under subsection 102B(q)(1) shall not preclude the certification required by proposed section 102(a) (dealing with electronic surveillance) or section 102A(a) (dealing with acquisition of foreign intelligence information by certain means other than electronic surveillance).

[35] The phrasing of the italicized portion of proposed section 102B(o) is somewhat unclear. Subsection 102B(o) states:

> If, pursuant to subsection (n), a United States district court determines that the acquisition *authorized under this section* was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived or otherwise grant the motion of the aggrieved person. If the court determines that such acquisition was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

[Emphasis added.] This may be a reference to Sec. 3(a) of H.R. 5825, although the context seems to suggest that the reference is to the section of FISA in which it occurs, that is new section 102B, rather than to the bill. However, it would appear that the "acquisition" referenced in new section 102B of FISA would not be authorized under section 102B, which deals with directives, but rather under new section 102A, if the acquisition of foreign intelligence information does not constitute electronic surveillance; and the acquisition requires the assistance of a wire or electronic communications provider, custodian, or other person who has access to wire or electronic communications, either as transmitted or as stored, or who has access to equipment that is being or may be used to transmit or store such communications.

As in subsection 102B(n), discussed in the previous footnote, there appears to be some uncertainty whether "acquisition" as used in subsection 102B(o) is intended to refer only to an acquisition of foreign intelligence information from a communications provider under subsection 102A, or whether it is also intended to encompass the gathering of information through an electronic surveillance under section 102. The broader interpretation might find some support from the heading of Sec. 3(a) of the bill as passed by the House, and from section 102B(q).

conducted, the court shall deny the aggrieved person's motion except to the extent that due process requires disclosure or discovery.[36]

Orders which grant motions or requests under proposed subsection 102B(n), decisions under section 102B that an electronic surveillance or an acquisition is not lawfully authorized or conducted, and U.S. district court orders requiring review or granting disclosure of directives, order, or other material related to an acquisition are final orders, binding on federal and state courts except a U.S. court of appeals and the U.S. Supreme Court.[37]

Proposed subsections 102B(i) through (p) appear similar, but not identical to current subsections 106(c) through (h) of FISA dealing with use of information derived from an electronic surveillance under title I of FISA.[38]

---

[36] Proposed subsection 102B(o) of FISA, Sec. 3(a) of H.R. 5825.

[37] Proposed subsection 102B(p) of FISA, Sec. 3(a) of H.R. 5825 .

[38] These subsections of current section 106 of FISA, 50 U.S.C. § 1806, provide:

> . . .
> (c) Notification by United States
> Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.
> (d) Notification by States or political subdivisions
> Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.
> (e) Motion to suppress
> Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that —
> (1) the information was unlawfully acquired; or
> (2) the surveillance was not made in conformity with an order of

(continued...)

Under proposed subsection 102B(q), federal officers who acquire foreign intelligence information may consult with federal law enforcement officers or state and local law enforcement personnel, including the chief executive officer of that state or political subdivision of the state with authority to appoint or direct the chief law enforcement officer of the state or political subdivision, to coordinate efforts to investigate or protect against three categories of circumstances: actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; sabotage, international terrorism, or the development or proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or clandestine intelligence activities by an intelligence service or network of a foreign power or by

---

[38] (...continued)

authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) In camera and ex parte review by district court

Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) Suppression of evidence; denial of motion

If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Finality of orders

Orders granting motions or requests under subsection (g) of this section, decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

an agent of a foreign power. Such coordination shall not preclude the Attorney General's certification required under proposed section 102 or 102A of FISA.[39]

Proposed subsection 102B(r) provides that a directive made or an order granted under new section 102B of FISA must be retained for not less than 10 years.

Sec. 3(b) of H.R. 5825 makes conforming amendments to the table of contents of FISA.

Sec. 4. Jurisdiction of FISA Court

Sec. 4 of H.R. 5825 amends section 103 of FISA, 50 U.S.C. § 1803, to add a new subsection 103(g) providing that applications for an FISC order authorizing electronic surveillance under title 1 of FISA are only authorized if the President, in a written authorization, has empowered the Attorney General to approve such applications. Under the proposed language, notwithstanding any other law, a judge to whom such an application is made may grant an order in conformity with section 105 of FISA, 50 U.S.C. § 1805, approving electronic surveillance of a foreign power or an agent of a foreign power to obtain foreign intelligence information.[40]

---

[39] This is similar but not identical to current subsection 106(k) of FISA, 50 U.S.C. § 1806. Subsection 106 applies to federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title, while subsection 102B(q)applies to federal officers who acquire foreign intelligence information. It might be argued that the latter has broader applicability, covering both those who acquire foreign intelligence information through electronic surveillance and those who do so by certain other means. This would seem to be consistent with the heading of Sec. 3 of H.R. 5825. It may also draw support from subsection 102B(q)(2) which indicates that coordination under paragraph 102B(q)(1) does not preclude the certification required by section 102(a) (which deals with electronic surveillance) or 102A(a) (which deals with acquisition of foreign intelligence information by certain other means).

Alternatively, it might be argued that, since "acquisition of foreign intelligence information" appears to be used as a term of art in proposed section 102A of FISA, that this section applies only to the latter. In support of this position, one might contend that, since the new provisions would be added to title I of FISA, subsection 106(k) by its terms might be read to apply to coordination where the foreign intelligence information is gathered by electronic surveillance under proposed section 102, as well as current sections 104 and 105 of FISA.

Proposed section 102B(q) differs from current section 106(k), in that section 102B(q) covers coordination of efforts to investigate or protect against the development or proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power, in addition to coordination for the other categories of investigative and protective efforts covered by both proposed section 102B(q) and current section 106(k).

[40] There appears to be some overlap of the first sentence of the proposed subsection 103(g) with parts of current section 104 of FISA, which requires, in pertinent part, that each application for a FISC order authorizing electronic surveillance to be approved by the Attorney General upon his finding, that the application satisfies the criteria and requirements for such an application set forth in title I of FISA, including a statement of the authority conferred on the Attorney General by the President of the United States and the approval

(continued...)

Sec. 5. Applications for Court Orders

Sec. 5 of H.R. 5825 amends some of the requirements for applications for court orders for electronic surveillance under section 104 of FISA, 50 U.S.C. § 1804. As amended by Sec. 5 of H.R. 5825, such an application must contain, among other requirements: a summary description of the nature of the information sought and the type of communications or activities to be subjected to the electronic surveillance;[41] and a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President to authorize electronic surveillance for foreign intelligence purposes[42] (a) that the certifying official deems the information sought to be foreign intelligence information, (b) that a significant purpose of the surveillance is to obtain foreign intelligence information, (c) that such information cannot reasonably be obtained by normal investigative techniques, and (d) including a statement of the basis for the certification that the information sought is the type of foreign intelligence information designated and that such information cannot reasonably be obtained by normal investigative techniques. As amended by Sec. 5 of the bill, such an application for a FISC order would also include a summary statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;[43] and a summary statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application. In addition, Sec. 5 of H.R. 5825 would require the application to contain a statement of the period of time for which the electronic surveillance is required to be maintained, and, if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this subchapter should not automatically terminate when the described type of

---

[40] (...continued)
of the Attorney General to make the application. The second sentence of the proposed subsection 103(g) appears to overlap somewhat with current subsection 103(a) of FISA, which creates the FISC, with jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth FISA.

[41] Under current section104(a)(6) of FISA, 50 U.S.C. § 1804(a)(6), an application for an FISC order authorizing electronic surveillance must contain a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance.

[42] Under current section 104(a)(7) of FISA, such certifications would be provided by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate.

[43] A requirement in current section 104(a)(7)(D) that an application for a FISC order authorizing electronic surveillance designate the type of foreign intelligence information being sought according to the categories described in section 101(e), 50 U.S.C. § 1801(e) would be deleted by Sec. 5(1)(B)(iii) of H.R. 5825 as passed by the House.

information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter.[44]

Current subsections 104(c) through (e) would be redesignated subsections 104(b) through (d) by Sec. 5(3) of H.R. 5825.[45] Current subsection 104(e),

---

[44] H.R. 5825, Sec. 5(1)(F), would strike a current requirement in subsection 104(a)(11) of FISA, 50 U.S.C. § 1804(a)(11), that, whenever more than one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, a section 104 application would include the coverage of the devices involved and what minimization procedures apply to information acquired by each device. H.R. 5825, Sec. 5(2), would strike current subsection 104(b) which excludes certain requirements from applications for electronic surveillance whenever the target of the electronic surveillance is a foreign power, as defined in section 101 (a)(1), (2), or (3), 50 U.S.C. § 1801(a)(1), (2), or (3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power; but would require a statement as to whether physical entry is required to effect the surveillance and shall contain such information about the surveillance techniques and communications or other information concerning United States persons likely to be obtained as may be necessary to assess the proposed minimization procedures.

[45] Current subsections 104(c), (d), and (e) of FISA, 50 U.S.C.§§ 1804(c), (d), and (e), provide:

> (c) Additional affidavits or certifications
>
> The Attorney General may require any other affidavit or certification from any other officer in connection with the application.
>
> (d) Additional information
>
> The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 105 [of FISA, 50 U.S.C. § 1805].
>
> (e) Personal review by Attorney General
>
> (1) (A) Upon written request of the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, or the Director of National Intelligence, the Attorney General shall personally review under subsection (a) of this section an application under that subsection for a target described in section 102(b)(2) [of FISA, 50 U.S.C. § 1801(b)(2)].
>
> (B) Except when disabled or otherwise unavailable to make a request referred to in subparagraph (A), an official referred to in that subparagraph may not delegate the authority to make a request referred to in that subparagraph.
>
> (C) Each official referred to in subparagraph (A) with authority to make a request under that subparagraph shall take appropriate actions in advance to ensure that delegation of such authority is clearly established in the event such official is disabled or otherwise unavailable to make such request.
>
> (2) (A) If as a result of a request under paragraph (1) the Attorney General determines not to approve an application under the second sentence of subsection (a) of this section for purposes of making the application under this section, the Attorney General shall provide written notice of the

(continued...)

redesignated subsection 104(d) by Sec. 5(3) of H.R. 5825, directs the Attorney General, upon request of the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, or the Director of National Intelligence, to personally review applications for a FISC order authorizing electronic surveillance under subsection 104(a) of a target who acts in the United States as an officer or employee of a foreign power, or as a member of a of a foreign power as defined in subsection (a)(4) of this section (that is, a group engaged in international terrorism or activities in preparation therefor). Sec. 5(4) of H.R. 5825 would expand the list of those whose request may trigger such personal review by the Attorney General to include the Director of the Central Intelligence Agency.

Sec. 6. Issuance of an Order

Sec. 6 of H.R. 5825 amends section 105 of FISA, 50 U.S.C. § 1805, dealing with the requirements for issuance of a FISC order for electronic surveillance.

Necessary Findings

Sec. 6(1) addresses provisions which deal with the necessary findings that a FISC judge must make in issuing an *ex parte* order approving an application for a court order authorizing electronic surveillance under Sec. 105 of FISA, 50 U.S.C. §

---

[45] (...continued)

> determination to the official making the request for the review of the application under that paragraph. Except when disabled or otherwise unavailable to make a determination under the preceding sentence, the Attorney General may not delegate the responsibility to make a determination under that sentence. The Attorney General shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event the Attorney General is disabled or otherwise unavailable to make such determination.
>
> (B) Notice with respect to an application under subparagraph (A) shall set forth the modifications, if any, of the application that are necessary in order for the Attorney General to approve the application under the second sentence of subsection (a) of this section for purposes of making the application under this section.
>
> (C) Upon review of any modifications of an application set forth under subparagraph (B), the official notified of the modifications under this paragraph shall modify the application if such official determines that such modification is warranted. Such official shall supervise the making of any modification under this subparagraph. Except when disabled or otherwise unavailable to supervise the making of any modification under the preceding sentence, such official may not delegate the responsibility to supervise the making of any modification under that preceding sentence. Each such official shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event such official is disabled or otherwise unavailable to supervise the making of such modification.

1805. Sec. 6(1)(A) of the bill would strike subsection 105(a)(1) of FISA.[46] Under Sec. 6(1)(B) of the bill, subsections 105(a)(2)-(5) of FISA would be redesignated subsections 105(a)(1)-(4) of FISA, respectively.

Specifications Required

Subsection 105(c)(1) of FISA currently requires that an order approving electronic surveillance under Section 105 of FISA must include certain specifications and sets out those specifications.[47] Sec. 6(2) of the bill would amend subsection

---

[46] Current section 105(a) of FISA, 50 U.S.C. § 1805(a), deals with the necessary findings that a FISC judge must make in an ex parte order approving an application under section 104 of FISA, 50 U.S.C. § 1804, authorizing electronic surveillance. Under current section 105(a)(1) of FISA, 50 U.S.C. § 1805(a)(1), the FISC judge must find, in part, that "the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information."

[47] Current section 105(c)(1) of FISA, 50 U.S.C. § 1805(c)(1), provides:

> (c) Specifications and directions of orders
>
> (1) Specifications
> An order approving an electronic surveillance under this section shall specify —
> (A) the identity, if known, or a description of the specific target of the electronic surveillance identified or described in the application pursuant to section 104(a)(3) [1804(a)(3) of this title];
> (B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known;
> (C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;
> (D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance;
> (E) the period of time during which the electronic surveillance is approved; and
> (F) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the devices involved and what minimization procedures shall apply to information subject to acquisition by each device.

As amended, subsection 105(c)(1) would provide:

> (c) Specifications and directions of orders
>
> (1) Specifications
> An order approving an electronic surveillance under this section shall specify —
> (A) the identity, if known, or a description of the specific target of the electronic surveillance identified or described in the application pursuant to section 104(a)(3) [1804(a)(3) of this title];
> (B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known;
> (C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

(continued...)

105(c)(1) of FISA to delete subsection 105(c)(1)(F), which currently requires that, whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, an order approving electronic surveillance under this section shall include the authorized coverage of the devices involved and what minimization procedures shall apply to information subject to acquisition by each device. This change is consistent with the deletion by H.R. 5825, Sec. 5(2) of a parallel requirement from the requirements for an application under section 104 of FISA.

Striking of Provision Dealing with Exclusion From FISA Electronic Surveillance Orders of Information Regarding Foreign Power Targets

Current subsection 105(d) of FISA, 50 U.S.C. § 1805(d), deals with exclusion of certain information respecting certain categories of foreign power targets from the *ex parte* order authorizing electronic surveillance under this section.[48] Sec. 6(3) of the bill strikes subsection 105(d) of FISA; and, under Sec. 6(4) of the bill, redesignates current subsections 105(e)-(i) of FISA, 50 U.S.C. §§ 1805(e)-(i), as new subsections 105(d)-(h) of FISA, 50 U.S.C. §§ 1805(d)-(h). This is consistent with the changes made by Sec. 5(2) of the bill to the requirements in section 104 of FISA for an application for a FISC order to authorize electronic surveillance.

---

[47] (...continued)

> (D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance; and
> (E) the period of time during which the electronic surveillance is approved.

[48] Current section 105(d) of FISA, 50 U.S.C. § 1805(d), provides:

> (d) Exclusion of certain information respecting foreign power targets
>
> Whenever the target of the electronic surveillance is a foreign power, as defined in section 101(a)(1), (2), or (3) [50 U.S.C. §1801(a)(1), (2), or (3)], and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the order need not contain the information required by subparagraphs (C), (D), and (F) of subsection (c)(1) of this section, but shall generally describe the information sought, the communications or activities to be subjected to the surveillance, and the type of electronic surveillance involved, including whether physical entry is required.

Subsections 101(a)(1), (2), or (3) of FISA, 50 U.S.C. §§ 1801(a)(1), (2), or (3) define "foreign power" to mean a foreign government or any component thereof, whether or not recognized by the United States; a faction of a foreign nation or nations, not substantially composed of United States persons; or an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments, respectively. Subparagraph 105(c)(1)(F), 50 U.S.C. §§ 1805(c)(1)(F), is deleted by Sec. 6(2)(C) of the bill.

Duration and Extension of Orders for Electronic Surveillance Under FISA

Current section 105(e) of FISA, 50 U.S.C. § 1805(e), which is redesignated by Sec. 6(4) of H.R. 5825 as section 105(d) of FISA, deals with duration of orders for electronic surveillance under FISA and conditions under which extensions to those orders may be granted by the FISC. Under that provision, an order for electronic surveillance generally may be for the duration described in the order or for 90 days, whichever is shorter. Current subsection 105(e)(1) (redesignated subsection 105(d)(1)) provides for two exceptions to this general rule. First, an order under section 105 of FISA shall approve an electronic surveillance targeted against a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title,[49] for the period specified in the application or for one year, whichever is less. Second, an order under FISA for a surveillance targeted against an agent of a foreign power who is not a United States person may be for the period specified in the application or for 120 days, whichever is less. Under current law, extensions are to be obtained in the same manner and upon the same type of findings as the original orders.

If the FISC judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period of the extension, then current law provides for and extension for up to a year of an order under for electronic surveillance under FISA targeted against a foreign power that is a foreign-based political organization not substantially composed of U.S. persons, an entity that is directed and controlled by a foreign government or governments, or a group engaged in international terrorism or activities in preparation therefor that is not a United States person. An extension of an order under FISA authorizing electronic surveillance targeted against an agent of a foreign power who is not a United States person may be for a period not to exceed one year.

Under subsection 6(5) of the bill, current subsection 105(e) of FISA (redesignated as subsection 105(d)(2) by Sec. 6(4) of H.R. 5825) would be amended to permit extensions for up to one year of an order issued under FISA to be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order.

Emergency Electronic Surveillance Prior to FISC Order

Under Sec. 6(6) of the bill, current subsection 105(f) of FISA, 50 U.S.C. § 1805(f) (redesignated by Sec. 6(4) of the bill as subsection 105(e)), is amended to provide authority for the Attorney General to authorize emergency employment of electronic surveillance if specific requirements are met. Under these requirements, the Attorney General must (1) determine that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained; (2) determine that the factual basis for issuance of an order under this title to approve such surveillance exists; (3) inform a FISC judge at the time of such authorization that the decision has been made to employ emergency electronic

---

[49] See footnote 42, *supra*.

surveillance; and (4) make an application in accordance with this title to a FISC judge, as soon as practicable, but not more than 168 hours (seven days) after the official authorizes such surveillance. Under current subsection 105(f) of FISA, the Attorney General's determinations in (1) and (2) above must be "reasonable," and an application for a FISC order authorizing the electronic surveillance must be made within 72 hours after the emergency electronic surveillance is authorized, rather than 168 hours as provided in the amended section under Sec. 6(6) of the bill. Sec. 6(6) also makes some non-substantive structural changes to the section.

As amended by Sec. 6(6) of the bill, redesignated subsection 105(e) of FISA also provides that, if the Attorney General authorizes such emergency employment of electronic surveillance, he must require that the minimization procedures required by this title for the issuance of a judicial order be followed. In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 168 hours from the time of authorization by the Attorney General, whichever is earliest. If such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person. A denial of the application made under this subsection may be reviewed as provided in section 103 of FISA, 50 U.S.C. § 1803. Under current law, in the absence of a court order approving the electronic surveillance, the surveillance must terminate when the information sought is obtained, when the application for an order is denied, or after the expiration of 72 hours from the time of authorization by the Attorney General, whichever is earlier. The provisions dealing with review of a denial of an application under this subsection and with limitations on use of the information gathered in an emergency electronic surveillance, where the application is denied or the surveillance is terminated and no court order approving the surveillance is issued, parallel those in current law.

Release From Liability

As amended by Sec. 6(7) of H.R. 5825, the redesignated subsection 105(h) of FISA (current subsection 105(i), 50 U.S.C. § 1805(i)) bars court action against any provider of an electronic communication service, landlord, custodian, or other person (including any officer, employee, agent or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under FISA for electronic surveillance or physical search; or in response to a certification by the Attorney General or a designee of the Attorney General seeking information, facilities, or technical assistance from such person under section 102B of FISA, 50 U.S.C. § 1802B.

Authorization of Pen Registers and Trap and Trace Devices Where Electronic Surveillance Involving Communications Authorized Under FISA

Sec. 6(8) of H.R. 5825 would add a new subsection 105(i) to FISA. Under this new provision, a FISC judge granting an application to conduct electronic surveillance involving communications would also have to authorize installation and use of pen registers and trap and trace devices to acquire dialing, routing, addressing, and signaling information related to such communications. The subsection further provides that such dialing, routing, addressing, and signaling information would not be subject to minimization procedures.

Sec. 7. Use of Information

Sec. 7 of the bill would amend subsection 106(i) of FISA, 50 U.S.C. § 1806(i), which deals with the destruction of information unintentionally acquired by an electronic, mechanical, or other surveillance device. The current provision covers such unintentional acquisition of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and an warrant would be required for law enforcement purposes, where the sender and all intended recipients are located within the United States. Under the current provision, the contents must be destroyed upon recognition, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

As amended by the bill, the provision covers such unintentionally acquired information from the contents of any communication, rather than being limited to the contents of radio communications. The new provision would permit retention of such unintentionally acquired information if the Attorney General determines that the contents contain significant foreign intelligence information or indicate a threat of death or serious bodily harm to any person.[50]

---

[50] Thus, the provision, as amended, would read:

> In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents contain significant foreign intelligence information or indicate a threat of death or serious bodily harm to any person.

Sec. 8. Congressional Oversight

Sec. 8 of H.R. 5825 makes several amendments to current congressional oversight provisions in section 108 of FISA, 50 U.S.C. § 1808, and in the National Security Act of 1947, as amended, 50 U.S.C. § 401 *et seq*. Section 108(a)(1) requires the Attorney General, on a semiannual basis, to fully inform the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, and the Senate Judiciary Committee concerning all electronic surveillance under Title I of FISA. Subsection 108(a)(1) further provides that nothing in Title I of FISA shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties.

Subsection 108(a)(2) of FISA, 50 U.S.C. § 1808(a)(2) sets out specific requirements for the contents of such reports. The amendment in Sec. 8 of the bill would add an additional requirement that the report include the authority under which the electronic surveillance is conducted.

Under current subsection 108(1)(b) of FISA, 50 U.S.C. § 1808(1)(b),

> On or before one year after October 25, 1978, and on the same day each year for four years thereafter, the Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence shall report respectively to the House of Representatives and the Senate, concerning the implementation of this chapter. Said reports shall include but not be limited to an analysis and recommendations concerning whether [FISA] should be (1) amended, (2) repealed, or (3) permitted to continue in effect without amendment.

This subsection would be repealed by the bill and replaced with a new subsection 108(1)(b), which would require the Attorney General, on a semiannual basis, also to "fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate on electronic surveillance conducted without a court order."

Sec. 8(b)(1) of H.R. 5825 amends the National Security Act of 1947, as amended, 50 U.S.C. § 401 *et seq*., to redesignate subsection 501(f), 50 U.S.C. § 413(f), as subsection 501(g) and to add a new subsection 501(f) which would provide that the Chair, in consultation with the respective ranking member, of each of the congressional intelligence committees, may inform, on a bipartisan basis, all members, or any individual members of such committee, and any essential committee staff, of a report submitted under subsection 501(a)(1) or (b), 50 U.S.C. §§ 413(a)(1) or (b),[51] as such Chair considers necessary.

---

[51] 50 U.S.C. § 413(a) and (b) provide:

> (a) Reports to Congressional committees of intelligence activities and anticipated activities
>
> (1) The President shall ensure that the congressional intelligence committees are

(continued...)

Sec.8(b)(2) of the bill amends section 502 of the National Security Act of 1947, as amended, 50 U.S.C. § 413a,[52] which provides reporting requirements for intelligence activities, other than covert actions, which are the responsibility of, are engaged in by, or are carried out for or on behalf of, any department, agency, or entity of the U.S. government, including any significant anticipated intelligence activity and any significant intelligence failure. Sec. 8(b)(2) of H.R. 5825 would add a new subsection 502(d),[53] which would provide that the Chair, in consultation with the respective ranking member, of each of the congressional intelligence committees, may inform, on a bipartisan basis, all members, or any individual members of such committee, and any essential committee staff, of a report submitted under subsection 502(a), 50 U.S.C. §§ 413a(a),[54] as such Chair considers necessary.

---

[51] (...continued)

> kept fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity as required by this subchapter.
>
> . . .
>
> (b) Reports concerning illegal intelligence activities
>
> The President shall ensure that any illegal intelligence activity is reported promptly to the congressional intelligence committees, as well as any corrective action that has been taken or is planned in connection with such illegal activity.

The term "intelligence activities" is defined in 50 U.S.C. § 413(f) to include "covert actions as defined in section 413b(e) of this title, and includes financial intelligence activities."

[52] The bill indicates that Section 502 of the National Security Act of 1947 as amended is 50 U.S.C. § 414. While 50 U.S.C. § 414, which deals with funding of intelligence activities, was formerly Section 502 of the National Security Act of 1947, as amended, it is now Section 504 of that Act. Section 502 of the National Security Act of 1947, as amended, is currently 50 U.S.C. § 413a.

[53] The proposed amendments appear substantively to be more consistent with the language of 50 U.S.C. § 413a than that of 50 U.S.C. § 414. While 50 U.S.C. § 413a has no subsection (d) under current law, 50 U.S.C. § 414, already has a subsection (d), which provides:

> (d) Report to congressional committees required for expenditure of nonappropriated funds for intelligence activity
>
> (1) Except as otherwise specifically provided by law, funds available to an intelligence agency that are not appropriated funds may be obligated or expended for an intelligence or intelligence-related activity only if those funds are used for activities reported to the appropriate congressional committees pursuant to procedures which identify —
>
> (A) the types of activities for which nonappropriated funds may be expended; and
>
> (B) the circumstances under which an activity must be reported as a significant anticipated intelligence activity before such funds can be expended.
>
> (2) Procedures for purposes of paragraph (1) shall be jointly agreed upon by the congressional intelligence committees and, as appropriate, the Director of National Intelligence or the Secretary of Defense.

[54] Current section 502(a), 50 U.S.C. § 413a(a), provides generally:

(continued...)

Subsection 8(b)(3) of H.R. 5825 would amend section 503 of the National Security Act of 1947, as amended, 50 U.S.C. § 413b,[55] which deals with presidential

---

[54] (...continued)

> To the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters, the Director of National Intelligence and the heads of all departments, agencies, and other entities of the United States Government involved in intelligence activities shall —
>
> > (1) keep the congressional intelligence committees fully and currently informed of all intelligence activities, other than a covert action (as defined in section 413b(e) of this title), which are the responsibility of, are engaged in by, or are carried out for or on behalf of, any department, agency, or entity of the United States Government, including any significant anticipated intelligence activity and any significant intelligence failure; and
> > (2) furnish the congressional intelligence committees any information or material concerning intelligence activities, other than covert actions, which is within their custody or control, and which is requested by either of the congressional intelligence committees in order to carry out its authorized responsibilities.

Current 50 U.S.C. § 414(a) provides:

> (a) Obligations and expenditures for intelligence or intelligence-related activity; prerequisites
> Appropriated funds available to an congressional intelligence committees may be obligated or expended for an intelligence or intelligence-related activity only if —
>
> > (1) those funds were specifically authorized by the Congress for use for such activities; or
> > (2) in the case of funds from the Reserve for Contingencies of the Central Intelligence Agency and consistent with the provisions of section 413b of this title concerning any significant anticipated intelligence activity, the Director of the Central Intelligence Agency has notified the appropriate congressional committees of the intent to make such funds available for such activity; or
> > (3) in the case of funds specifically authorized by the Congress for a different activity —
> >
> > > (A) the activity to be funded is a higher priority intelligence or intelligence-related activity;
> > > (B) the need for funds for such activity is based on unforseen [FN1] requirements; and
> > > (C) the Director of National Intelligence, the Secretary of Defense, or the Attorney General, as appropriate, has notified the appropriate congressional committees of the intent to make such funds available for such activity;
>
> > (4) nothing in this subsection prohibits obligation or expenditure of funds available to an intelligence agency in accordance with sections 1535 and 1536 of Title 31.

[55] The bill refers to 50 U.S.C. § 415, which was formerly section 503 of the National Security Act of 1947, as amended. That provision deals with notice to Congress of certain transfers of defense articles and defense services. However, the current section 503 of the (continued...)

approval and reporting of covert actions, to add a new subsection 503(g). The new subsection would provide that the Chair, in consultation with the respective ranking member, of each of the congressional intelligence committees, may inform, on a bipartisan basis, all members, or any individual members of such committee, and any essential committee staff, of a report submitted under subsection 503(b), (c), or (d), as such Chair considers necessary.[56]

---

[55] (...continued)
National Security Act of 1947, as amended, is 50 U.S.C. § 413b.

[56] Current subsections 503(b), (c), and (d) of the National Security Act of 1947, 50 U.S.C. § 413b(b), (c), and (d), provide:

> (b) Reports to congressional intelligence committees; production of information
> To the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters, the Director of National Intelligence and the heads of all departments, agencies, and entities of the United States Government involved in a covert action —
>
> (1) shall keep the congressional intelligence committees fully and currently informed of all covert actions which are the responsibility of, are engaged in by, or are carried out for or on behalf of, any department, agency, or entity of the United States Government, including significant failures; and
> (2) shall furnish to the congressional intelligence committees any information or material concerning covert actions which is in the possession, custody, or control of any department, agency, or entity of the United States Government and which is requested by either of the congressional intelligence committees in order to carry out its authorized responsibilities.
>
> (c) Timing of reports; access to finding
>
> (1) The President shall ensure that any finding approved pursuant to subsection (a) of this section shall be reported to the congressional intelligence committees as soon as possible after such approval and before the initiation of the covert action authorized by the finding, except as otherwise provided in paragraph (2) and paragraph (3).
> (2) If the President determines that it is essential to limit access to the finding to meet extraordinary circumstances affecting vital interests of the United States, the finding may be reported to the chairmen and ranking minority members of the congressional intelligence committees, the Speaker and minority leader of the House of Representatives, the majority and minority leaders of the Senate, and such other member or members of the congressional leadership as may be included by the President.
> (3) Whenever a finding is not reported pursuant to paragraph (1) or (2) of this section [FN1], the President shall fully inform the congressional intelligence committees in a timely fashion and shall provide a statement of the reasons for not giving prior notice.
> (4) In a case under paragraph (1), (2), or (3), a copy of the finding, signed by the President, shall be provided to the chairman of each congressional intelligence committee. When access to a finding is limited to the Members of Congress specified in paragraph (2), a statement of the reasons for limiting such access shall also be provided.
>
> (d) Changes in previously approved actions

(continued...)

Sec. 9. International Movement of Targets

Electronic Surveillance Under FISA

Sec. 9(a) of H.R. 5825, would amend current section 105(e) of FISA, 50 U.S.C. § 1805(e) (which is redesignated to be section 105(d) of FISA by Sec. 6(4) and amended by Sec. 6(5) of the bill), by adding a new subsection (4). The new subsection would require an order issued under section 105 of FISA, 50 U.S.C. § 1805, to remain in force during the authorized period of surveillance notwithstanding the absence of the target from the United States, unless the government files a motion to extinguish the order and the court grants that motion.

Physical Searches Under FISA

Sec. 9(b) of H.R. 5825, would amend section 304(d) of FISA, 50 U.S.C. § 1824(d), to add a new subsection 304(d)(4) of FISA. The new subsection would require an order issued under 304(d) of FISA to remain in force "during the authorized period of surveillance [sic?][57] notwithstanding the absence of the target

---

[56] (...continued)

> The President shall ensure that the congressional intelligence committees, or, if applicable, the Members of Congress specified in subsection (c)(2) of this section, are notified of any significant change in a previously approved covert action, or any significant undertaking pursuant to a previously approved finding, in the same manner as findings are reported pursuant to subsection (c) of this section.

Under subsection 503(e) of the National Security Act of 1947, as amended, 50 U.S.C. § 413b(e), "covert action" is defined to mean:

> an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include —
>
> (1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;
>
> (2) traditional diplomatic or military activities or routine support to such activities;
>
> (3) traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or
>
> (4) activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad.

[57] As this section deals not with electronic surveillance but with physical searches under FISA, it seems possible that the term "surveillance" may have been intended to read "physical search."

from the United States, unless the Government files a motion to extinguish the order and the court grants the motion."

Sec. 10. Compliance with Court Orders and Antiterrorism Programs

This section of the bill limits liability for a set period of time for those who assist the government between September 11, 2001 and 60 days after enactment of the bill, while acting in compliance with FISC orders or antiterrorism programs. Sec. 10(a) states:

> (a) In General- Notwithstanding any other provision of law, and in addition to the immunities, privileges, and defenses provided by any other provision of law, no action, claim, or proceeding shall lie or be maintained in any court, and no penalty, sanction, or other form of remedy or relief shall be imposed by any court or any other body, against any person[58] for an activity arising from or relating to the provision to an element of the intelligence community[59] of any information (including records or other information pertaining to a customer), facilities, or assistance during the period of time beginning on September 11, 2001, and ending on the date that is 60 days after the date of the enactment of this Act, in connection with any alleged communications intelligence program that the Attorney General or a designee of the Attorney General certifies, in a manner

---

[58] Under subsection 10(c)(2) of H.R. 5825, the term "person" is defined by reference to 18 U.S.C. § 2510(6) to mean "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation."

[59] Under subsection 10(c)(1) of H.R. 5825, the term "intelligence community" is defined by reference to section 3(4) of the National Security Act of 1947, 50 U.S.C. § 401a(4) to include:

> (A) The Office of the Director of National Intelligence.
> (B) The Central Intelligence Agency.
> (C) The National Security Agency.
> (D) The Defense Intelligence Agency.
> (E) The National Geospatial-Intelligence Agency.
> (F) The National Reconnaissance Office.
> (G) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs.
> (H) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Federal Bureau of Investigation, and the Department of Energy.
> (I) The Bureau of Intelligence and Research of the Department of State.
> (J) The Office of Intelligence and Analysis of the Department of the Treasury.
> (K) The elements of the Department of Homeland Security concerned with the analysis of intelligence information, including the Office of Intelligence of the Coast Guard.
> (L) Such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

> consistent with the protection of State secrets, is, was, or would be intended to protect the United States from a terrorist attack. This section shall apply to all actions, claims, or proceedings pending on or after the effective date of this Act.

Subsection 10(b) would make any action, claim, or proceeding described in subsection 10(a) that is brought in a state court removable to federal court under 28 U.S.C. § 1441 as arising under the Constitution and laws of the United States.[60]

Sec. 11. Report on Minimization Procedures

Sec. 11(a) of the bill requires, within two years of enactment of the measure, and annually thereafter until December 31, 2009, submission of a report to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence by the Director of the National Security Agency, in consultation with the Director of National Intelligence and the Attorney General, on the effectiveness and use of minimization procedures applied to information concerning United States persons acquired during the course of a communications activity conducted by the National Security Agency. Subsection 11(b) provides that such reports must include a description of the implementation, during the course of communications intelligence activities conducted by the National Security Agency, of procedures established to minimize the acquisition, retention, and dissemination of nonpublicly available information concerning United States persons; the number of significant violations, if any, of such minimization procedures during the 18 months following the effective date of this Act; and summary descriptions of such violations. Under subsection 11(c) of the bill, information concerning United States persons should not be retained solely for the purpose of complying with the reporting requirements of this section.

Sec. 12. Authorization After an Armed Attack

Warrantless Electronic Surveillance for Limited Period Under FISA

Notwithstanding any other provision of law, under current section 111 of FISA, 50 U.S.C. § 1811, the President, through the Attorney General, may authorize electronic surveillance without a court order under FISA to acquire foreign intelligence information for a period not to exceed 15 calendar days following a declaration of war by the Congress.

---

[60] 28 U.S.C.A. § 1441(b) provides:

> (b) Any civil action of which the district courts have original jurisdiction founded on a claim or right arising under the Constitution, treaties or laws of the United States shall be removable without regard to the citizenship or residence of the parties. Any other such action shall be removable only if none of the parties in interest properly joined and served as defendants is a citizen of the State in which such action is brought.

Subsection 12(a) of H.R. 5825 would amend this section to provide that, notwithstanding any other provision of law, the President, through the Attorney General, may authorize electronic surveillance without a court order under FISA to acquire foreign intelligence information "for a period not to exceed 90 days following an armed attack against the territory of the United States if the President submits to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate notification of the authorization under this section."

Warrantless Physical Search for Limited Period Under FISA

Notwithstanding any other provision of law, under current section 309 of FISA, 50 U.S.C. § 1829, the President, through the Attorney General, may authorize physical searches without a court order under FISA to acquire foreign intelligence information for a period not to exceed 15 calendar days following a declaration of war by the Congress.

Subsection 12(b) of H.R. 5825 would amend this section to provide that, notwithstanding any other provision of law, the President, through the Attorney General, may authorize physical searches without a court order under FISA to acquire foreign intelligence information "for a period not to exceed 90 days following an armed attack against the territory of the United States if the President submits to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate notification of the authorization under this section."

Sec. 13. Authorization of Electronic Surveillance After a Terrorist Attack

Initial Authorization

Sec. 13 of H.R. 5825 would add a new section 112 to FISA, dealing with authorization of electronic surveillance following a terrorist attack upon the United States, and makes conforming amendments to the FISA table of contents. Under the new subsection 112(a), for a period of up to 90 days following a terrorist attack against the United States, the President, acting through the Attorney General, may authorize electronic surveillance without an FISC order to acquire foreign intelligence information if the President submits a required notification to the congressional intelligence committees[61] and to a judge having jurisdiction under section 103 of FISA.[62] That notification must advise the recipients that the United

---

[61] The term "congressional intelligence committees" is defined under proposed section 112(h) of FISA to mean the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence.

[62] This phrase might be viewed as open to more than one interpretation. Section 103 of FISA, 50 U.S.C. § 1803, establishes what has come to be known as the Foreign Intelligence

(continued...)

States has been the subject of a terrorist attack and must identify the terrorist organizations or affiliates of terrorist organizations believed to be responsible for the terrorist attack.

Subsequent Certifications

Under Sec. 13 of H.R. 5825, Subsection 112(b) of FISA would give the President the authority to continue electronic surveillance for subsequent 90 day periods upon submission of successive certifications to the congressional intelligence committees and to a judge having jurisdiction under section 103 of FISA that the circumstances of the terrorist attack for which the President submitted a certification under subsection (a) require the President to continue the authorization of electronic surveillance under this section for an additional 90 days.

Electronic Surveillance of Individuals

Proposed subsection 112(c) of FISA gives particular attention to electronic surveillance of individuals. Under this subsection, the President, or an official designated by the President to authorize electronic surveillance, may only conduct electronic surveillance of a person under this section if the President or such official determines that there is a reasonable belief that such person is communicating with a terrorist organization or an affiliate of a terrorist organization that is reasonably believed to be responsible for the terrorist attack, and that the information obtained from the electronic surveillance may be foreign intelligence information.

---

[62] (...continued)
Surveillance Court (FISC), made up of 11 U.S. district court judges from seven of the U.S. judicial circuits publicly designated by the Chief Justice of the United States. Under section 103(a) of FISA, 50 U.S.C. § 1803(a), this court is given jurisdiction to hear applications and to grant orders authorizing electronic surveillance anywhere in the United States under FISA. Under subsection 103(b) of FISA, 50 U.S.C. § 1803(b), the Foreign Intelligence Surveillance Court of Review (Court of Review) is established, made up of three U.S. district court or U.S. court of appeals judges publicly designated by the Chief Justice of the United States. Subsection 103(b) gives this court jurisdiction to review the denial of any application made FISA. If such court determines that the application was properly denied, the court shall immediately provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision. Thus, "a judge having jurisdiction under section 103" of FISA may refer to either an FISC judge or a Court of Review judge. Judges of both of these courts could be said to "hav[e] jurisdiction under section 103."

Although perhaps less persuasive, it might be argued that this language may be broad enough to encompass a Supreme Court Justice, as that Court is also given jurisdiction over review of Court of Review decisions approving a denial of an application for an FISC order approving electronic surveillance under FISA. In addition, it might be noted that FISC judges have authority to act individually to review and grant applications for court orders approving electronic surveillance under FISA, while the Court of Review appears to issue decisions as a panel. One might argue, therefore, that notice to an FISC judge might be intended here.

Minimization Procedures

Proposed subsection 112(d) prohibits the President from authorizing electronic surveillance under this section until the Attorney General approves minimization procedures for such electronic surveillance.

Electronic Surveillance of United States Persons

Under proposed subsection 112(e), notwithstanding subsections 112(a) or (b), the President may not authorize electronic surveillance of a United States person[63] under section 112 of FISA for a period of more than 60 days without an FISC order approving such electronic surveillance under title I of FISA, unless the President, acting through the Attorney General, submits a certification to the congressional intelligence committees that four criteria are met. The President, acting through the Attorney General, must certify that the continued electronic surveillance of the United States person is vital to the national security of the United States. The certification must describe the circumstances that have prevented the Attorney General from obtaining an order under this title for continued surveillance. It must also describe the reasons for believing the United States person is affiliated with or in communication with a terrorist organization or affiliate of a terrorist organization that is reasonably believed to be responsible for the terrorist attack. Finally, it must describe the foreign intelligence information derived from the electronic surveillance conducted under section 112.

Use of Information

Subsection 112(f) would permit information obtained pursuant to electronic surveillance "under this subsection" [sic?][64] to be used to obtain an order authorizing subsequent electronic surveillance under Title I of FISA.

Reporting Requirements

Subsection 112(g) requires the President, within 14 days of submission of a certification under subsection 112(a), and every 30 days thereafter until he ceases to authorize electronic surveillance under subsections 112(a) or (b), to submit to the congressional intelligence committees a report on the electronic surveillance conducted under this section, including a description of each target of electronic surveillance under this section; and the basis for believing that each target is in communication with a terrorist organization or an affiliate of a terrorist organization.

---

[63] See fn. 1, *supra*, for the FISA definition of "United States person."

[64] This may be intended to read "section" rather than "subsection."

Sec. 14. Authorization of Electronic Surveillance Due to Imminent Threat

Sec. 14 of H.R. 5825 would add a new section 113 to the end of Title I of FISA providing for authorization of electronic surveillance to acquire foreign intelligence information for up to 90 days without a court order based upon a presidential determination that an imminent threat exists of attack likely to cause death, serious injury, or substantial economic damage to the United States. Notification to the congressional leadership and the congressional intelligence committees and to the FISC would be required. Subsequent extensions for up to 90 days at a time based upon new certifications would be possible. It would also make conforming amendments to the table of contents of FISA.

Initial Authorization

Under proposed subsection 113(a) of FISA, notwithstanding any other provision of law, but subject to the provisions of new section 113, the President, through the Attorney General, may authorize electronic surveillance without an FISC order to acquire foreign intelligence information for a period not to exceed 90 days if the President submits to the congressional leadership,[65] the congressional intelligence committees,[66] and the Foreign Intelligence Surveillance Court a written notification that the President has determined that there exists an imminent threat of attack likely to cause death, serious injury, or substantial economic damage to the United States. The notification, which may be in classified form, must be submitted as soon as practicable, but no later than five days after the date on which the President authorizes electronic surveillance under this section. It must specify the entity responsible for the threats and any affiliates of the entity, state the reason to believe that the threat of imminent attack exists, state the reason the President needs broader authority to conduct electronic surveillance in the United States as a result of the threat of imminent attack, and include a description of the foreign intelligence information that will be collected and the means that will be used to collect it.

Subsequent Authorizations

Under proposed subsection 113(b), at the end of the original 90-day period, and every 90 days thereafter, the President may submit a subsequent written notification to the congressional leadership, the congressional intelligence committees, the other relevant committees,[67] and the FISC that the circumstances of the threat for which the

---

[65] Under proposed subsection 113(g)(2) of FISA, the term "congressional leadership" is defined to mean "the Speaker and minority leader of the House of Representatives and the majority leader and minority leader of the Senate."

[66] Under proposed subsection 113(g)(1) of FISA, the term "congressional intelligence committees" is defined to mean "the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate."

[67] Under subsection 113(g)(4), the term "other relevant committees" is defined to mean "the (continued...)

President submitted a written notification under subsection 113(a) require the President to continue the authorization of electronic surveillance under this section for an additional 90 days. After each such notification, the President shall be authorized to conduct electronic surveillance under this section for an additional 90 days.

Electronic Surveillance of Individuals

New subsection 113(c) of FISA would permit the President, or an official designated by the President, to authorize electronic surveillance, to conduct electronic surveillance of an individual under this section only if specific requirements are satisfied. The President or the designated official must determine that "there is a reasonable belief that such person is communicating with an entity or an affiliate of an entity that is reasonably believed to be responsible for imminent threat of attack;" and "the information obtained from the electronic surveillance may be foreign intelligence information."

Minimization Procedures

Electronic surveillance under this section may not be authorized by the President unless the Attorney General approves applicable minimization procedures.

Electronic Surveillance of United States Persons

Notwithstanding subsections 113(a) and (b), the President may not authorize electronic surveillance of a U.S. person[68] under this section without an FISC order under Title I of FISA for a period of more than 60 days, unless the President, acting through the Attorney General, submits a certification to the congressional intelligence committees that meets four criteria. He must certify that the continued electronic surveillance of the United States person is vital to the national security of the United States. The certification must also describe the circumstances that have prevented the Attorney General from obtaining an order under this title for continued surveillance; describe the reasons for believing the United States person is affiliated with or in communication with an entity or an affiliate of an entity that is reasonably believed to be responsible for imminent threat of attack; and describe the foreign intelligence information derived from the electronic surveillance conducted under this section.

Use of Information Acquired by Electronic Surveillance Under This Section

Information obtained "under this subsection [sic?] may be used to obtain an order authorizing subsequent electronic surveillance" under Title I of FISA.

---

[67] (...continued)
Committees on Appropriations, the Committees on Armed Services, and the Committees on the Judiciary of the House of Representatives and the Senate."

[68] For the FISA definition of "United States person," see fn. 1, *supra.*

Sec. 15. Technical and Conforming Amendments

Sec. 15 makes a number of technical and conforming amendments to FISA, all of which are related to changes discussed earlier. Section 105(a)(4) of FISA, 50 U.S.C. § 1805(a)(4) is amended to replace "104(a)(7)(E)" with "104(a)(7)(D)" and to replace "104(d) with "104(c)," both changes reflecting redesignation of the affected sections under Sec. 6(1)(B) of H.R. 5825. In section 106(j) of FISA, in the matter preceding paragraph (1), "105(d)" would be replaced with "105(e)," reflecting changes made by Sec. 6(3) of H.R. 5825. Finally, "105(f)" would be replaced with "105(e)" in section 108(a)(2)(C) of FISA, 50 U.S.C. § 1808(a)(2)(C), to make the latter consistent with redesignation of specific subsections in section 105 of FISA, 50 U.S.C. § 1805, by Sec. 6(3) of the bill.